Encryption Scanner 2.0.x Manual

Tech Assist Inc.
1835A South Center City Parkway #414
Escondido, CA 92025
support@encryptionscanner.com
760 489-9282 v

Introduction

Thank You for purchasing the Encryption Scanner 2.0.
The Encryption Scanner is NOT an anti-malware, anti-virus, anti-ransomware removal tool. Encryption Scanner is an "inside the perimeter" alerting tool, which sends emails and reports when it detects that folders or files designated by you have become encrypted.

Encryption Scanner 2.0 fills the gap left by major anti-virus software companies that presume to protect you from an encryption-virus attack.

Encryption Scanner is based on the notion that all efforts to protect your computers will – at some point— fail, and hackers will find a way into your system, encrypting your files. IF THEY DO – the Encryption Scanner will be there to alert you to the fact that your protection-system has failed and you can take immediate action to protect yourself.

As of this time Q3 of 2015, there is nothing like Encryption Scanner on the market. But why? The reason is: a software detection system that runs inside a protected perimeter is based on the idea that the perimeter will fail. No anti-virus software maker is willing to admit there is a CHANCE a hacker will get passed their software. To admit that, is to admit failure. But don't worry – Encryption Scanner is here.

Encryption Scanner will detect and test against these common file types that are infected by encryption viruses: .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .csv, .pdf, .jpg, .png

What the Encryption Scanner 2.0 can do for you in a nutshell.

The Encryption Scanner 2.0 is better than version 1.x which only ran from the System Tray. Encryption Scanner 2.0 gives you the option of choosing to manually scan folders and files from the System Tray Icon or to run as a Windows Service in the background.

Running Encryption Scanner as a Windows Service, Encryption Scanner constantly checks to see if any folder or file(s) have been or are encrypted. If you wish to use Encryption Scanner as a manual checking tool, simply install and open the app from the System Tray [choose Display], and input the path to the folder or file you want to have checked. Click Start. A report will be generated.

Also from the System Tray, right-click on the "ES" icon and open the service configuration interface to setup the Encryption Scanner Windows Service, the location of the folders to be checked, the timer repeat cycle and the list of email addresses where reports are to be sent in the event of an attack.

Open the Options button by right-clicking the System Tray icon to perform several configuration settings, such as desktop alerts, or to turn off the timer.

Installation

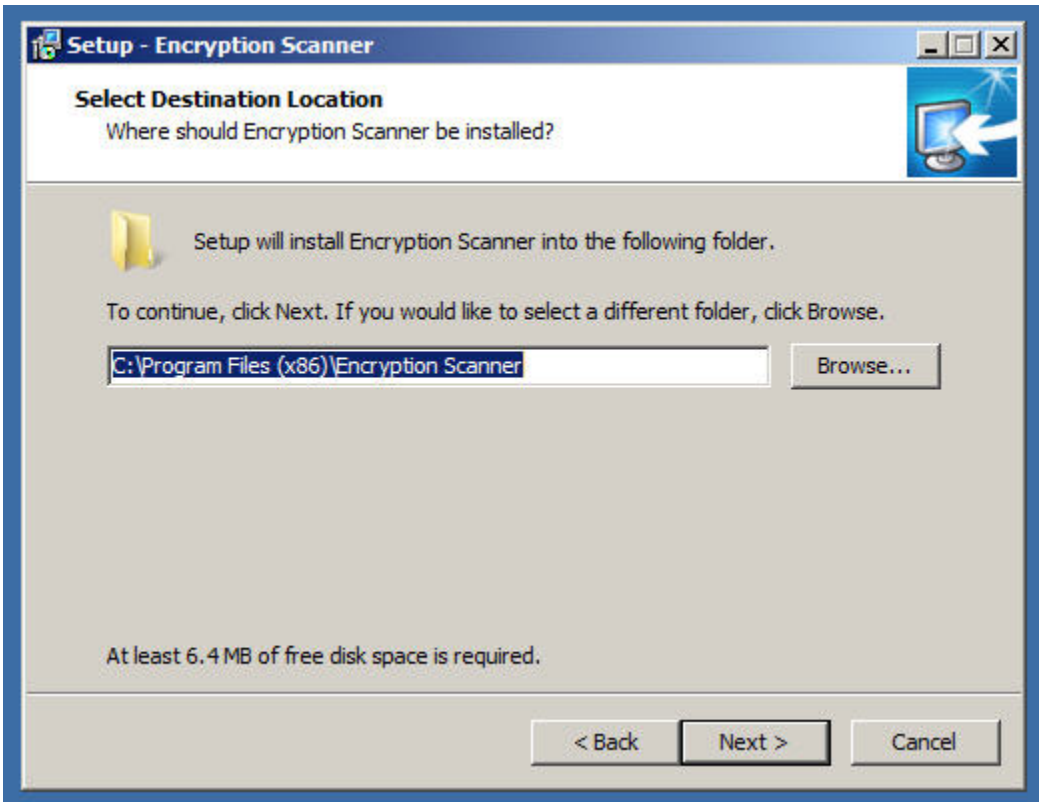
1. After downloading the Encryption Scanner 2.0 application compressed ZIP file, place the file in your downloads folder, your desktop, or wherever it is convenient for you. You can also place the file on a network share if you need to install Encryption Scanner 2.0 on multiple machines. Be sure to adhere to licensing requirements for multi-computer deployments.
    a. **Note:** Shut down or temporarily disable all anti-virus and anti-malware on your PC before installing Encryption Scanner.
2. After file placement in the downloads folder:
    a. Use a Windows or other utility to extract the file contents from the ZIP file.
    b. Launch or RUN the SETUP.EXE file.
    c. The Setup Wizard will open; click Next
    d.
Setup - Encryption Scanner
Welcome to the Encryption Scanner Setup Wizard
This will install Encryption Scanner version 2.0.0 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel
    e. Read and approve the Software License Agreement, then click Next.

f.

Setup - Encryption Scanner
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
Software License Agreement
1. This is an agreement between Tech Assist Inc., a California Corporation and Licensee, who is being licensed to use the Encryption Scanner software.
2. Licensee acknowledges that this is only a limited nonexclusive license. Tech Assist Inc., a California Corporation is and remains the owner of all titles, rights, and interests in the Encryption Scanner.
3. This License permits Licensee to install the Software [also known herein as the Encryption Scanner] on more than one computer system, as long as
I accept the agreement
I do not accept the agreement
< Back
Next >
Cancel

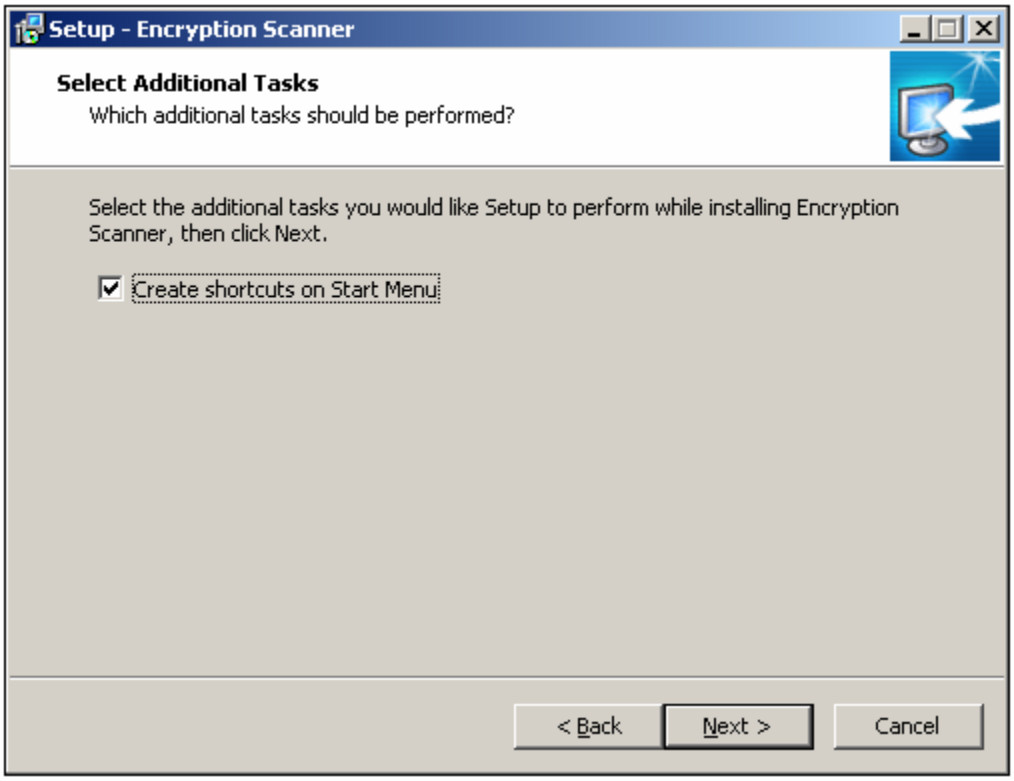
g. Select the destination for the Encryption Scanner application. In most cases, simply take the default.

h.


Setup - Encryption Scanner
Select Destination Location
Where should Encryption Scanner be installed?
Setup will install Encryption Scanner into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files (x86)\Encryption Scanner
Browse...
At least 6.4 MB of free disk space is required.
< Back
Next >
Cancel

i. Select to accept the shortcuts on the Start menu. Encryption Scanner will be installed into the System Tray in the lower-right area of your Windows desktop. There will be NO DESKTOP icon unless you choose to create one manually. Encryption Scanner's features can be managed solely from the System tray.

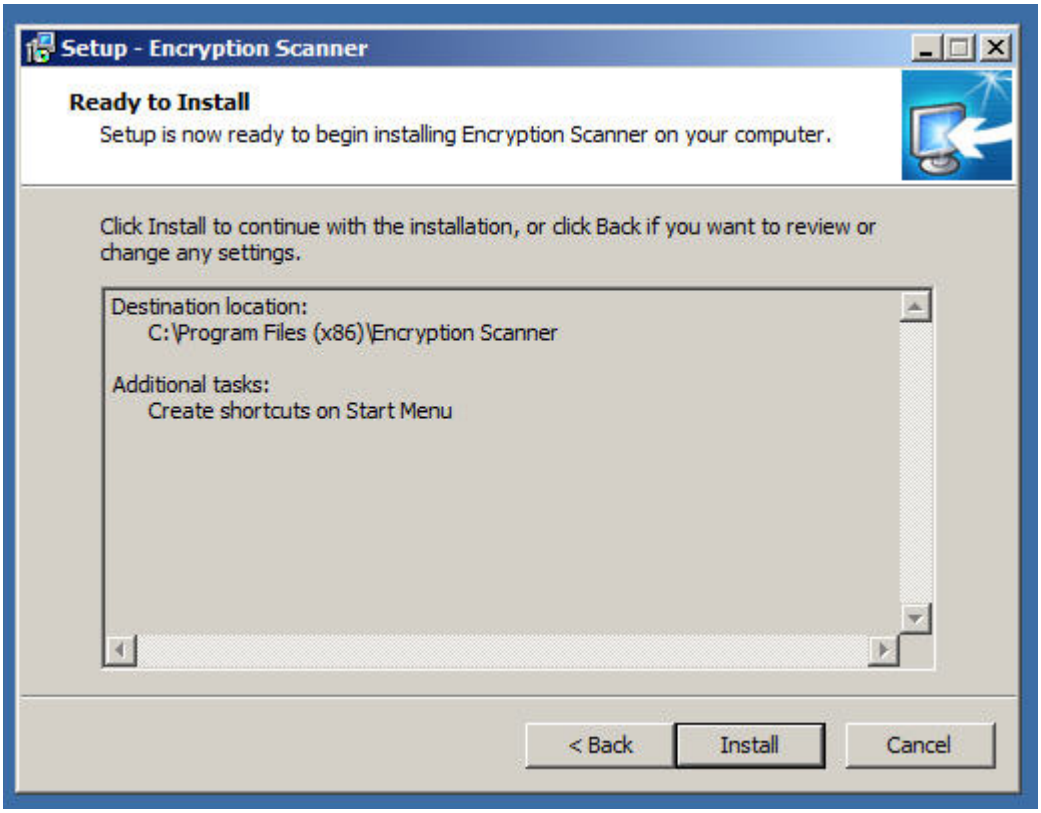
j.


Setup - Encryption Scanner
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing Encryption Scanner, then click Next.
Create shortcuts on Start Menu
< Back
Next >
Cancel

k. You are now Ready to Install. Click Next. Encryption Scanner will install onto your computer.

   i. NOTE: If you are installing on **Windows XP** you may need to install **.NET Framework 2.0** first before installing Encryption Scanner. See the Troubleshooting section at the end of this manual for more details and a download location for .NET Framework 2.0

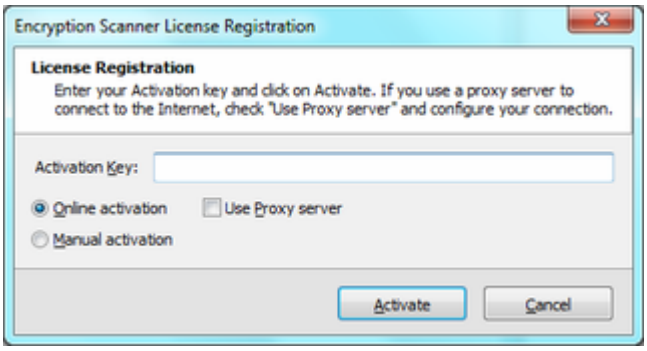
l.


Setup - Encryption Scanner
Ready to Install
Setup is now ready to begin installing Encryption Scanner on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files (x86)\Encryption Scanner
Additional tasks:
Create shortcuts on Start Menu
< Back
Install
Cancel

m. In some cases—like with Windows XP, Windows 2003 Server or other x32 operating systems, you may be prompted to reboot your computer. Close all other applications and reboot your computer to complete the install If you are not prompted run the Encryption Scanner application.

n.

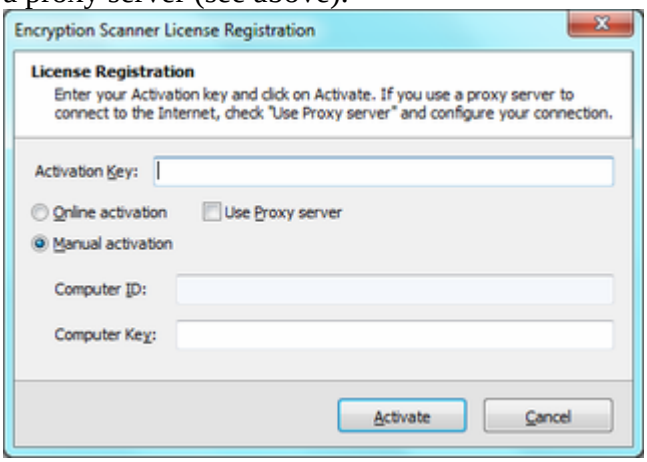
3. Your default installation of Encryption Scanner 2.0 comes with a free fully functional 15-day trial period. After you run the Encryption Scanner 2.0 for 15 days you will need to either uninstall the app or buy a registration license. The Encryption Scanner 2.0 License Registration box can be seen by right clicking the Encryption Scanner system tray app and choosing Activate/Register.

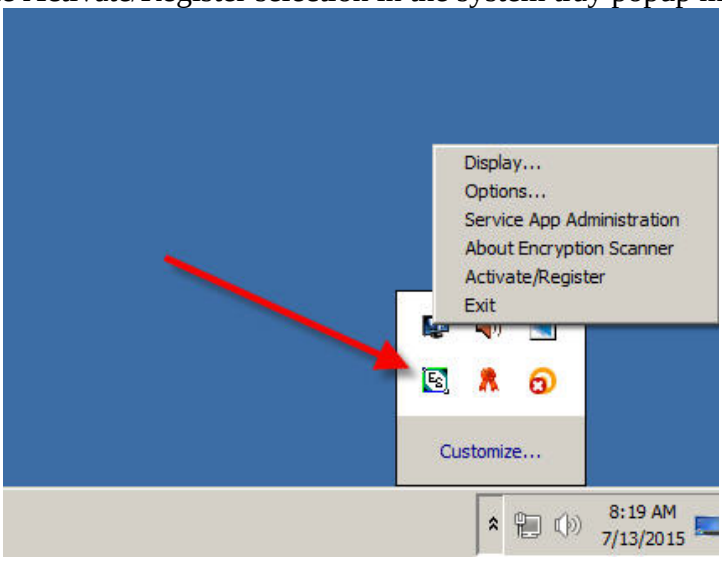
a. 
Encryption Scanner License Registration
License Registration
Enter your Activation key and click on Activate. If you use a proxy server to connect to the Internet, check "Use Proxy server" and configure your connection.
Activation Key:
Online activation
Use Proxy server
Manual activation
Activate
Cancel

b. Use the default “Online Activation” choice for inserting your Activation Code you acquired when purchasing Encryption Scanner to register your product for use (see above).

c.

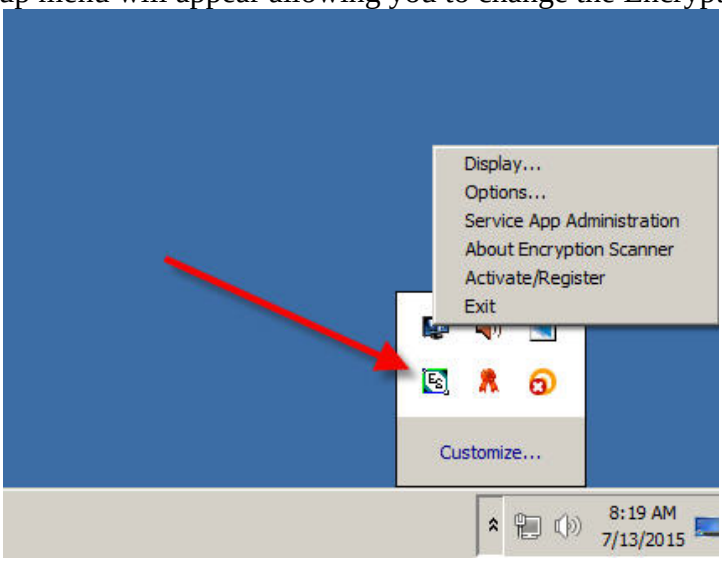
d. Use the “Use Proxy Server” selection to register your activation if you need to login through a proxy server (see above).

e. 
Encryption Scanner License Registration
License Registration
Enter your Activation key and click on Activate. If you use a proxy server to connect to the Internet, check "Use Proxy server" and configure your connection.
Activation Key:
Online activation
Use Proxy server
Manual activation
Computer ID:
Computer Key:
Activate
Cancel

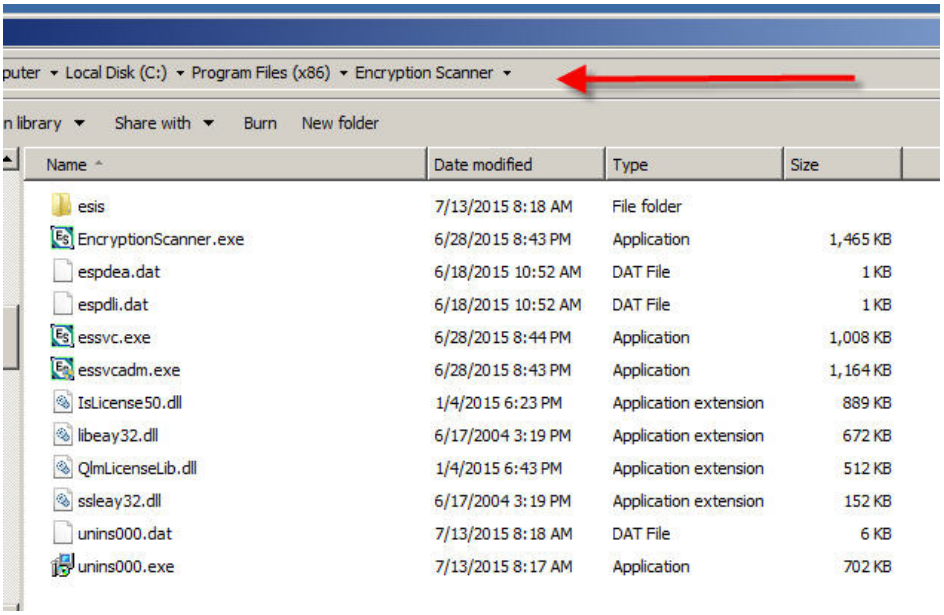
f. Use the “Manual Activation” if online-access to the internet is unavailable but you still have your Computer Key activation code.
g. IF YOU ARE USING THE TRIAL VERSION KEYS and want to manually register your license, click on the Activate/Register selection in the system tray popup menu.
h. 

4. When you start your computer after activation, Encryption Scanner 2.0 will be running in the System Tray. Access to its features is obtained by RIGHT-CLICKING on the Encryption Scanner icon.
   a. **NOTE: Encryption Scanner 2.0 is both a Windows SERVICE and a manual application. To access the Encryption Scanner 2.0 Windows Service configuration setup ONLY, see the next section.**

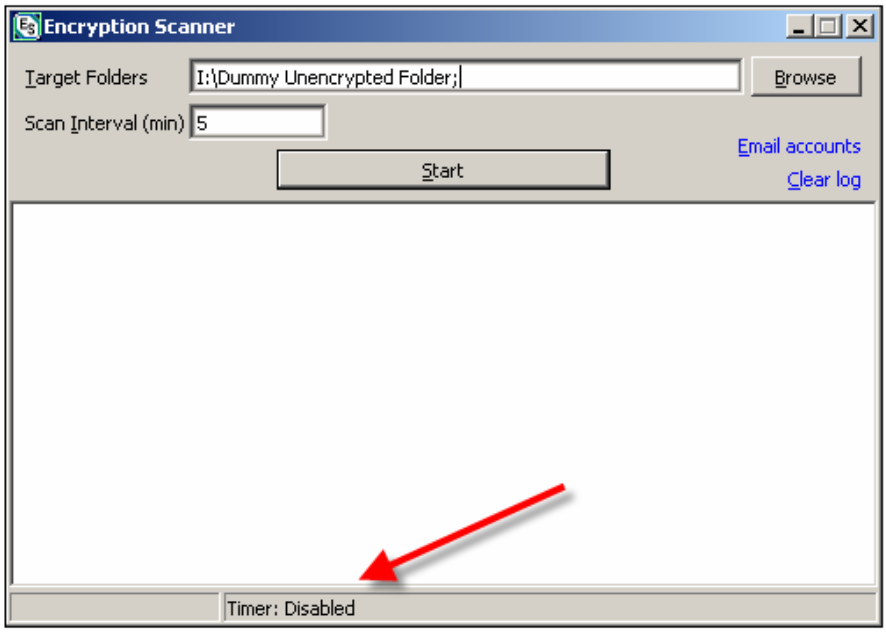
MANUAL DISPLAY CONFIGURATION

5. A Pop-up menu will appear allowing you to change the Encryption Scanner configuration features.
a. 

6. Clicking the DISPLAY… will open the Encryption Scanner 2.0 MANUAL app.
   a. The manual-app is the application you can use to manually scan files and folders for encrypted files and generate reports on those scans.
   b. If you don’t like using the System Tray - Display, you can create your own desktop icon by creating a Windows Shortcut based the file EncryptionScanner.exe located in the Encryption Scanner program files path.

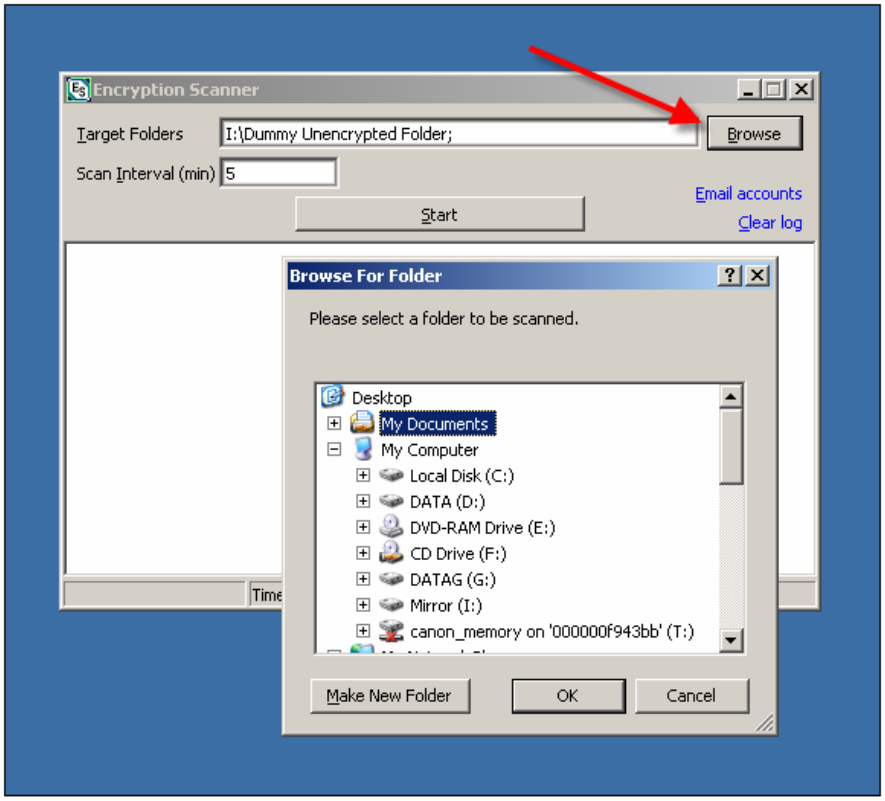
c. 
puter ▸ Local Disk (C:) ▸ Program Files (x86) ▸ Encryption Scanner
n library ▾ Share with ▾ Burn New folder
Name Date modified Type Size
esis 7/13/2015 8:18 AM File folder
EncryptionScanner.exe 6/28/2015 8:43 PM Application 1,465 KB
espdea.dat 6/18/2015 10:52 AM DAT File 1 KB
espdli.dat 6/18/2015 10:52 AM DAT File 1 KB
essvc.exe 6/28/2015 8:44 PM Application 1,008 KB
essvcadm.exe 6/28/2015 8:43 PM Application 1,164 KB
IsLicense50.dll 1/4/2015 6:23 PM Application extension 889 KB
libeay32.dll 6/17/2004 3:19 PM Application extension 672 KB
QlmLicenseLib.dll 1/4/2015 6:43 PM Application extension 512 KB
ssleay32.dll 6/17/2004 3:19 PM Application extension 152 KB
unins000.dat 7/13/2015 8:18 AM DAT File 6 KB
unins000.exe 7/13/2015 8:17 AM Application 702 KB

d. The EncryptionScanner.exe launches the Display window, which looks like this (see below). Use the Display app for manual scans and reports.

e. 

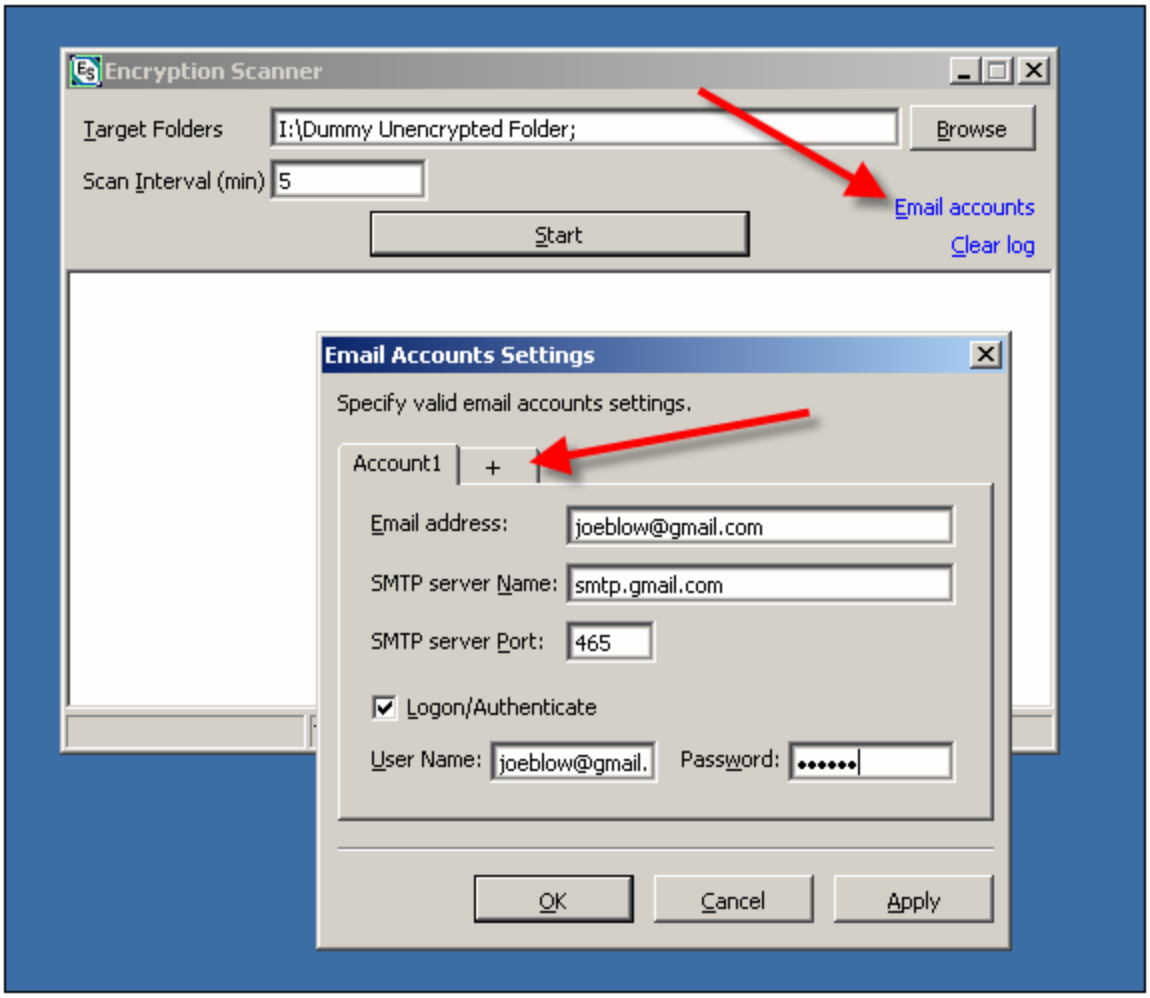
7. Here is a description of the manual Display fields and buttons:
   a. TARGET FOLDERS – This is where you assign the folders and files you wish to have scanned.
   b. TIMER: - After the initial installation, the Timer is Disabled until the user clicks the START button. Then the TIMER starts scanning at the intervals set in the SCAN INTERVAL (MIN) field.
   c. SCAN INTERVAL (MIN) – Set the interval in minutes between automatic scans of the Targeted folders

d.

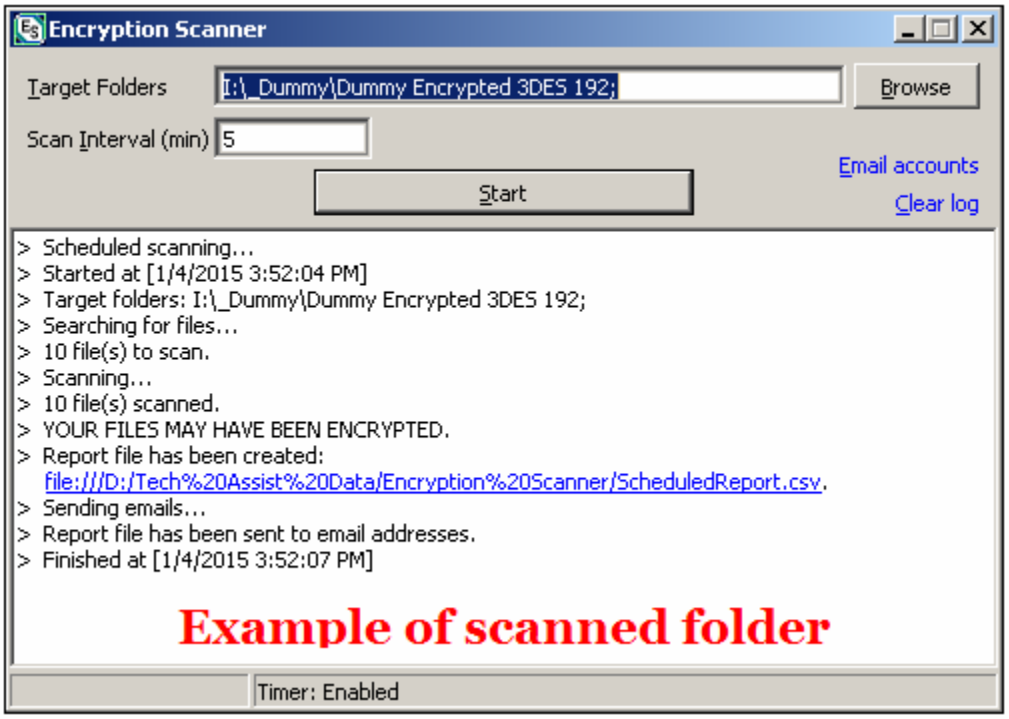


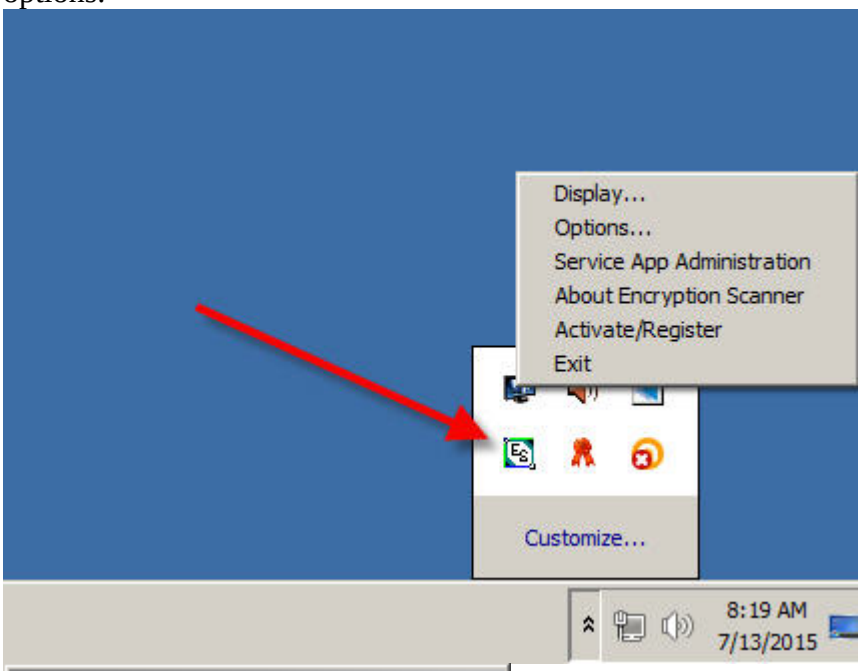
e. BROWSE – This is the standard Windows file-manager method of searching for a folder path. Multiple folder-paths are separated by SEMI-COLONS. A SEMI-COLON must be at the end of the path string.

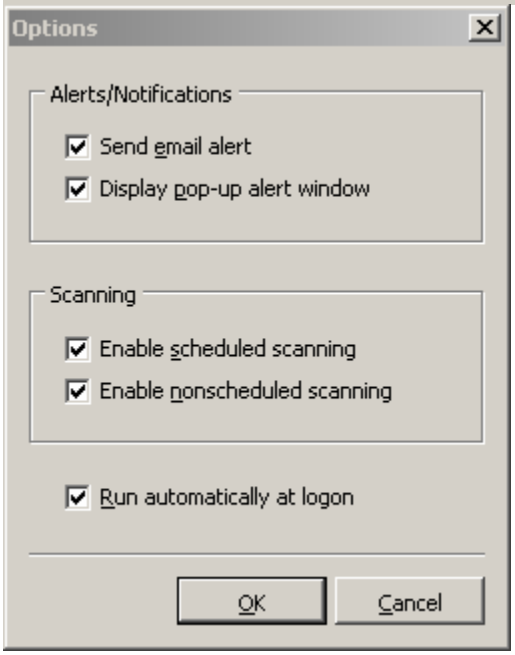
f. EMAIL ACCOUNTS – This blue-link opens the configuration area where you can setup your email notification information, to include email address, SMTP authentication, and other information.

g. 

h. CLEAR LOG – Clear Log clears the Big White field in the center of the application where reports information is generated at each scan.

i. 

8. MANUAL DISPLAY OPTIONS
    a. From the POPUP systems tray icon, click Options to configure the manual Display app options.
    b. 



    c. The OPTIONS boxes allows you to customize the Encryption Scanner manual Display app behavior. It DOES NOT configure the SERVICE options. Service options are configured in the Service Admin interface.
    d. Check – Uncheck the “Send email alert” to send or not send email alerts
    e. Check – Uncheck the “Display pop-up alert window” to use a pop-up alert when encrypted files are found.
    f. The “Enable scheduled scanning” and Enable nonscheduled scanning” boxes are mutually exclusive when one of them is unchecked.
        i. NOTE 1: A “timer-based scan” and a manual scan started by clicking the Start button on the main display are considered “Scheduled scans.” Therefore, if you uncheck "Enable Scheduled scanning", timer based and manual scans are disabled.

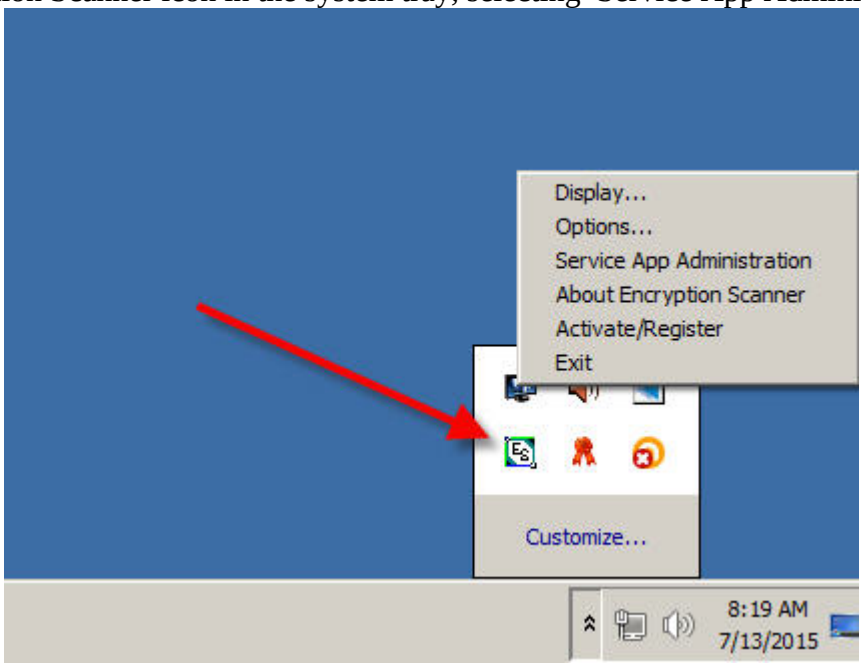
ii. NOTE 2: The “timer” is enabled only when target folders text field AND scan interval text field are NOT empty AND "Enable Scheduled scanning" is checked. A "Nonscheduled" scan is started implicitly when any file in one of the target folders is changed. This change may have been made by that user if he has worked on his files, or by any other background programs. Results of this scan are shown only if the scanned file is found as encrypted.

g. Check – Uncheck the “Run automatically at logon” to keep Encryption Scanner running after a restart of your computer. Encryption Scanner is not a background-service. You must logon to a Windows desktop session to run Encryption Scanner. This is to assist Encryption Scanner in writing reports and tracking folder paths.

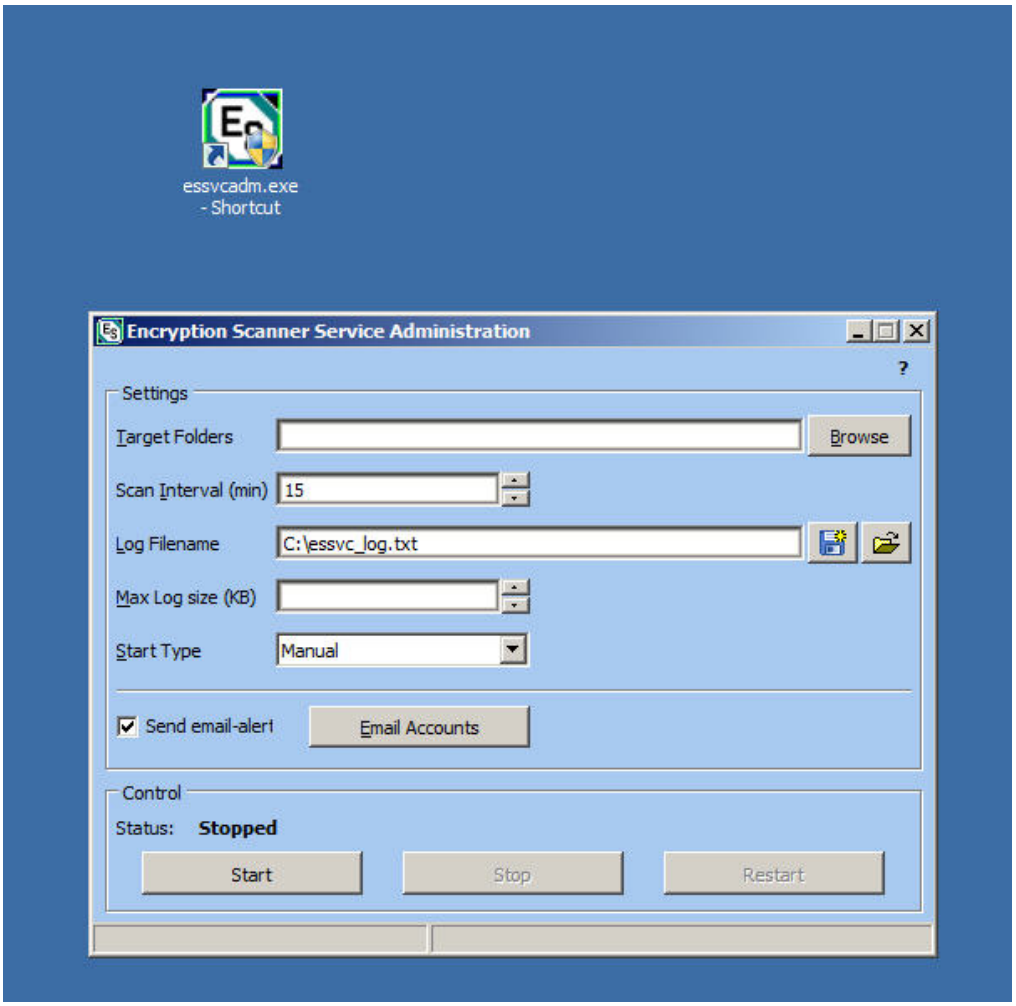
SERVICE APP ADMINISTRATION

Encryption Scanner 2.0 allows you to run Encryption Scanner as a Windows Service. Here is how to configure the Encryption Scanner 2.0 as a Windows Service.

1. Access the Encryption Scanner 2.0 Service App Administraion interface by right-clicking the Encryption Scanner icon in the system tray, selecting Service App Administration:

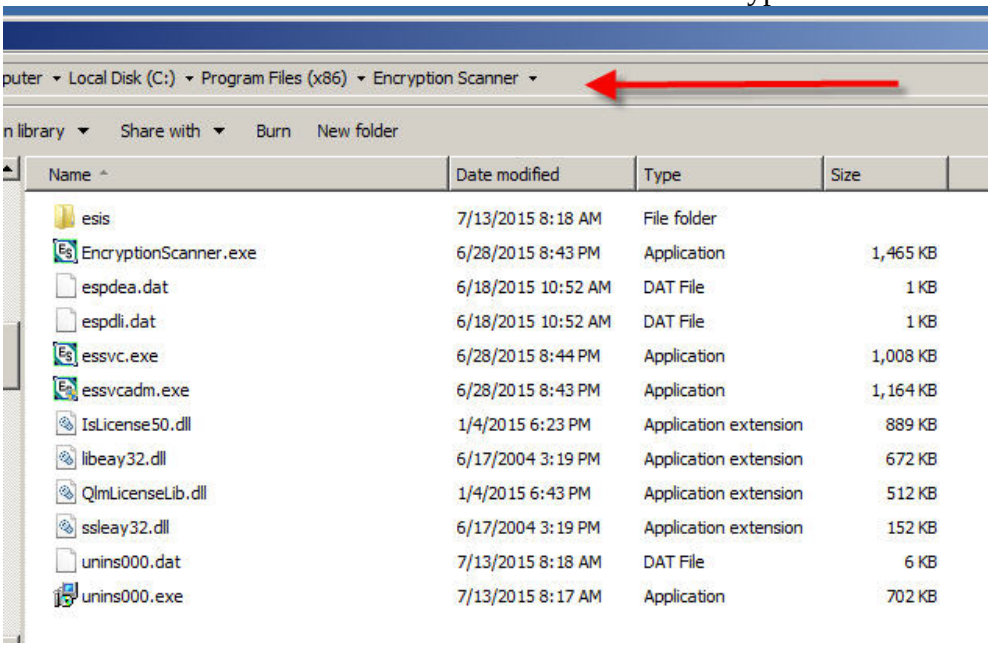


a.
b. The Service App Administration interface will open
c. Optionally you can create a desktop shortcut icon to the Encryption Scanner 2.0 Service App Administraion interface.



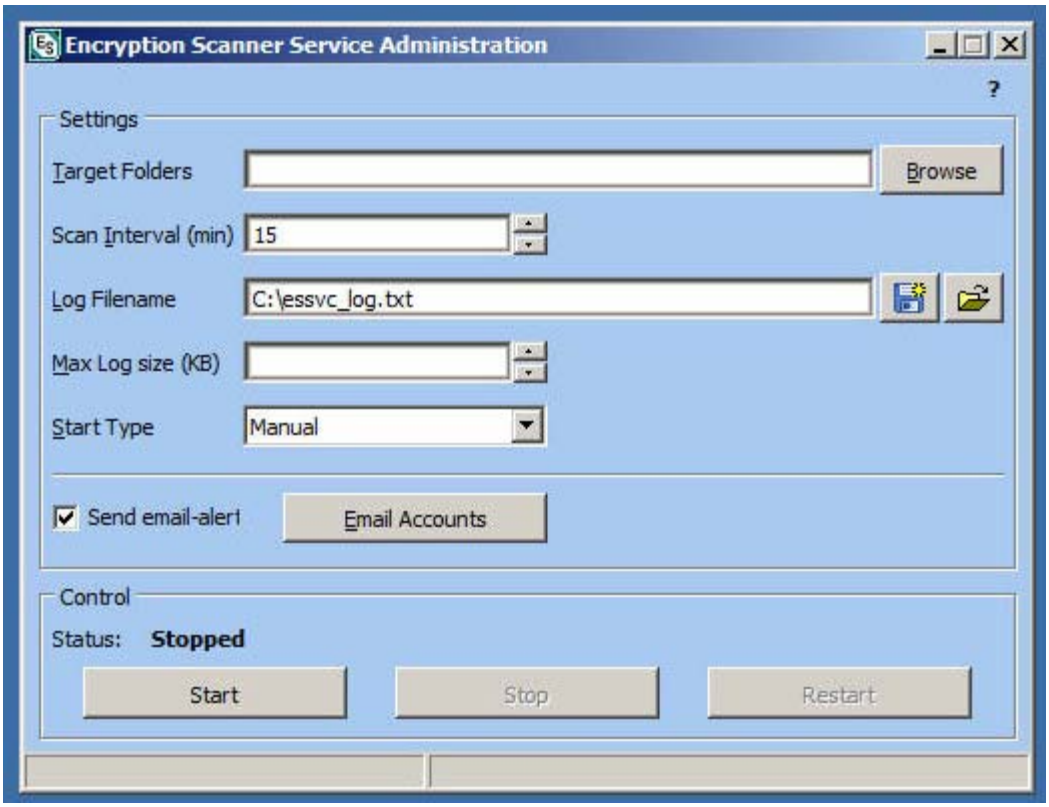
d.

e. The Service App Administration icon can be created by creating a shortcut icon from the EXE file known as ESSVCADM.EXE located in the Encryption Scanner 2.0 path.


puter ▸ Local Disk (C:) ▸ Program Files (x86) ▸ Encryption Scanner ▸
n library ▾ Share with ▾ Burn New folder
Name
Date modified
Type
Size
esis 7/13/2015 8:18 AM File folder
EncryptionScanner.exe 6/28/2015 8:43 PM Application 1,465 KB
espdea.dat 6/18/2015 10:52 AM DAT File 1 KB
espdli.dat 6/18/2015 10:52 AM DAT File 1 KB
essvc.exe 6/28/2015 8:44 PM Application 1,008 KB
essvcadm.exe 6/28/2015 8:43 PM Application 1,164 KB
IsLicense50.dll 1/4/2015 6:23 PM Application extension 889 KB
libeay32.dll 6/17/2004 3:19 PM Application extension 672 KB
QlmLicenseLib.dll 1/4/2015 6:43 PM Application extension 512 KB
ssleay32.dll 6/17/2004 3:19 PM Application extension 152 KB
unins000.dat 7/13/2015 8:18 AM DAT File 6 KB
unins000.exe 7/13/2015 8:17 AM Application 702 KB

f.

g. The Service App Administration interface is described as follows:

i. 

ii. TARGET FOLDERS / BROWSE: Used to point to a single or multiple folder location where the service will scan for encrypted files.

iii. SCAN INTERVAL (min): This is the number of minutes you would like between scan intervals. The default is 15 minutes

iv. LOG FILENAME. This is the path and location of the log file where reports are stored.

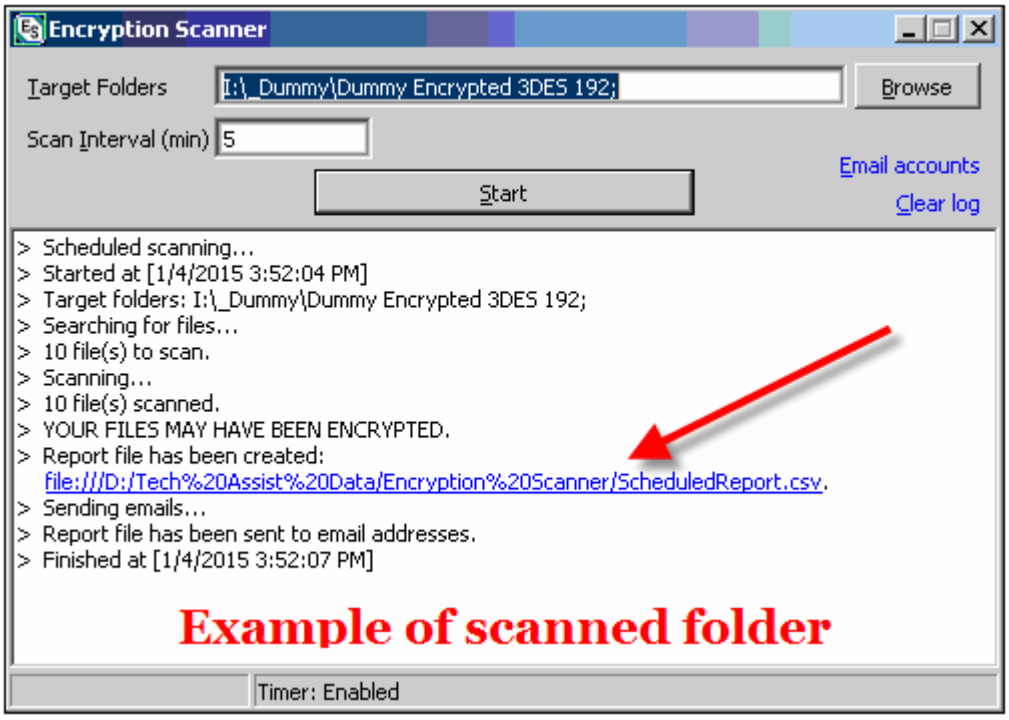
v. MAX LOG SIZE (KB). This is the maximum allowed log file size, which auto-truncated. We recommend 2048 as a min log file size for starters.

vi. START TYPE. This is same drop down box used in the Windows Services console to set a service to run automatically, automatically with delay, run manually, or be disabled.

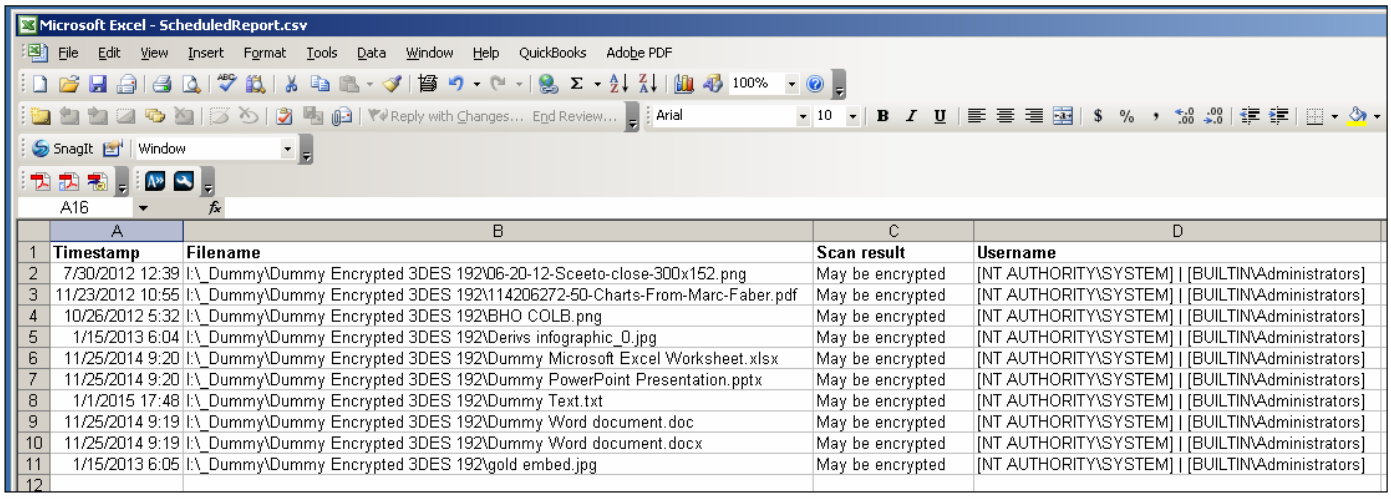
vii. SEND EMAIL ALERTS and Email Accounts button. The check box turns on or off the email alert sub-routine. If set to off, only the log collects scan results. They are not emailed unless the box is checked. The Email Accounts button allows you to setup multiple email addresses to which scan results are emailed. Email passwords are encrypted internally within Encryption Scanner 2.0.

viii. CONTROL – STATUS - Start, Stop, Restart. Just like in the Windows Services console, this sets the service to start (if off), Stop the service if it is running, and restart the service if it is running.

LOOKING AT A REPORT IN THE DISPLAY

1. 

   a. After a report is generated, the DISPLAY interface shows a similar response as shown above. Click on the LINK in blue in the Encryption Scanner report box and if you have Microsoft© Excel or some other spreadsheet program available to open a CSV [comma delimited] file, you can see the details of the report. See example next slide below:

2. 

	A	B	C	D
1	Timestamp	Filename	Scan result	Username
2	7/30/2012 12:39	I:_Dummy\Dummy Encrypted 3DES 192\06-20-12-Sceeto-close-300x152.png	May be encrypted	[NT AUTHORITY\SYSTEM] | [BUILTIN\Administrators]
3	11/23/2012 10:55	I:_Dummy\Dummy Encrypted 3DES 192\114206272-50-Charts-From-Marc-Faber.pdf	May be encrypted	[NT AUTHORITY\SYSTEM] | [BUILTIN\Administrators]
4	10/26/2012 5:32	I:_Dummy\Dummy Encrypted 3DES 192\BHO COLB.png	May be encrypted	[NT AUTHORITY\SYSTEM] | [BUILTIN\Administrators]
5	1/15/2013 6:04	I:_Dummy\Dummy Encrypted 3DES 192\Derivs infographic_0.jpg	May be encrypted	[NT AUTHORITY\SYSTEM] | [BUILTIN\Administrators]
6	11/25/2014 9:20	I:_Dummy\Dummy Encrypted 3DES 192\Dummy Microsoft Excel Worksheet.xlsx	May be encrypted	[NT AUTHORITY\SYSTEM] | [BUILTIN\Administrators]
7	11/25/2014 9:20	I:_Dummy\Dummy Encrypted 3DES 192\Dummy PowerPoint Presentation.pptx	May be encrypted	[NT AUTHORITY\SYSTEM] | [BUILTIN\Administrators]
8	1/1/2015 17:48	I:_Dummy\Dummy Encrypted 3DES 192\Dummy Text.txt	May be encrypted	[NT AUTHORITY\SYSTEM] | [BUILTIN\Administrators]
9	11/25/2014 9:19	I:_Dummy\Dummy Encrypted 3DES 192\Dummy Word document.doc	May be encrypted	[NT AUTHORITY\SYSTEM] | [BUILTIN\Administrators]
10	11/25/2014 9:19	I:_Dummy\Dummy Encrypted 3DES 192\Dummy Word document.docx	May be encrypted	[NT AUTHORITY\SYSTEM] | [BUILTIN\Administrators]
11	1/15/2013 6:05	I:_Dummy\Dummy Encrypted 3DES 192\gold embed.jpg	May be encrypted	[NT AUTHORITY\SYSTEM] | [BUILTIN\Administrators]
12				

Sample Dummy Folders with Dummy Files

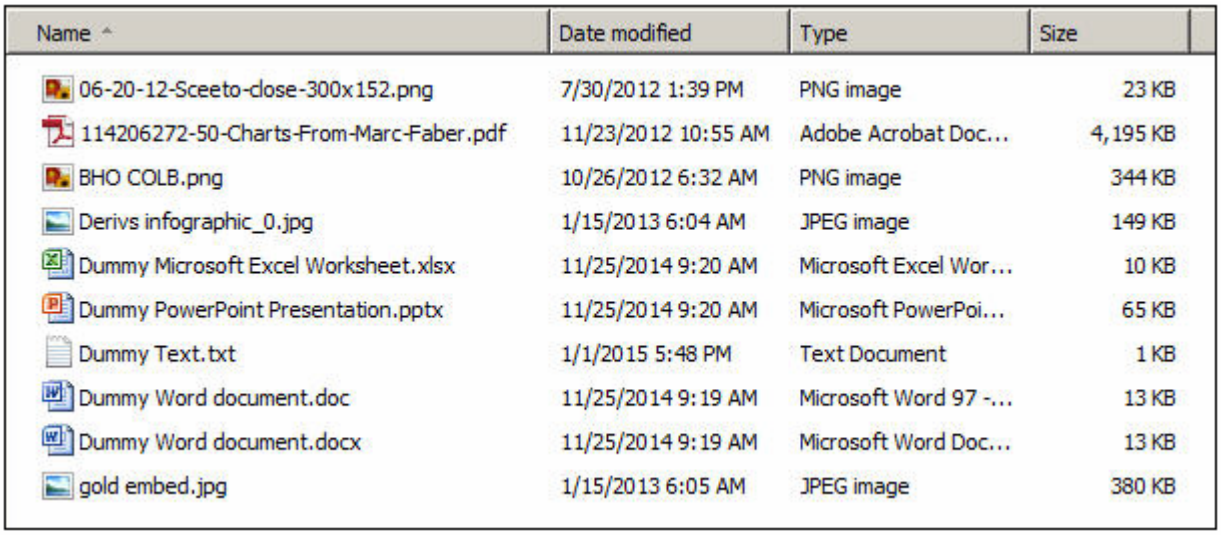
When using the new Encryption Scanner 2.0 as a Windows Service, we recommend that you use our "dummy" files as a "trap" for any encryption virus that infects your target machine. You can use your own set of files and folders, of course (it doesn't matter which ones you use.) But it is a good idea to establish a dummy-target of files. By doing so, the Encryption Scanner will not have to scan large numbers of files on every timer-cycle, thus using up server resources unnecessarily.

The Username of the last authorized user to 'change' the file is listed in the report – helping you to isolate and identify which user may be the "carrier" of the virus on your network. The file name and path is also listed helping you identify which exact files have been encrypted—and by inference, determine which files have NOT been encrypted. This feature alone saves you hours of time in tracking the damage down with your network.

We have provided some dummy files and folders of both encrypted and unencrypted files, which you can use to practice setting up and running Encryption Scanner scans and reports. Look for the downloads on our website in the SUPPORT section.

How to Use The Dummy Files

We have supplied on our website a download of some unencrypted files that you can use to setup your own "Crypto-virus trap."

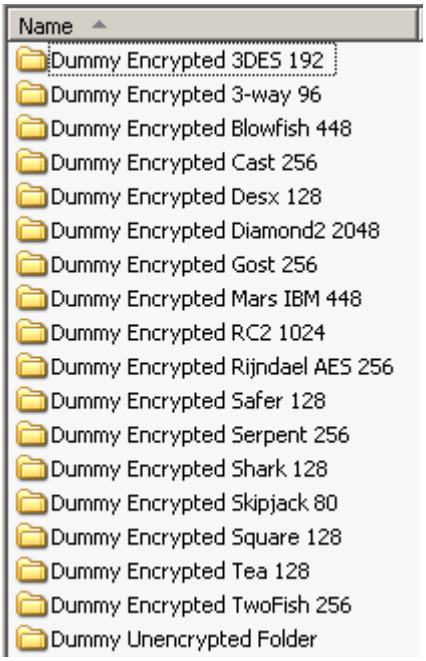


Name	Date modified	Type	Size
06-20-12-Sceeto-close-300x152.png	7/30/2012 1:39 PM	PNG image	23 KB
114206272-50-Charts-From-Marc-Faber.pdf	11/23/2012 10:55 AM	Adobe Acrobat Doc...	4,195 KB
BHO COLB.png	10/26/2012 6:32 AM	PNG image	344 KB
Derivs infographic_0.jpg	1/15/2013 6:04 AM	JPEG image	149 KB
Dummy Microsoft Excel Worksheet.xlsx	11/25/2014 9:20 AM	Microsoft Excel Wor...	10 KB
Dummy PowerPoint Presentation.pptx	11/25/2014 9:20 AM	Microsoft PowerPoi...	65 KB
Dummy Text.txt	1/1/2015 5:48 PM	Text Document	1 KB
Dummy Word document.doc	11/25/2014 9:19 AM	Microsoft Word 97 -...	13 KB
Dummy Word document.docx	11/25/2014 9:19 AM	Microsoft Word Doc...	13 KB
gold embed.jpg	1/15/2013 6:05 AM	JPEG image	380 KB

WARNING: IF YOU DECIDE TO USE YOUR OWN DUMMY FILES--- first ensure that they are not encrypted. Then make a practice scan using Encryption Scanner 2.0. Some GIF files may register as a "false positive" in Encryption Scanner 2.0, since we have expanded the Encryption Scanner 2.0 capabilities to examine a larger set of digital components within targeted files.

After you download the ZIPed file from our support page and unzip the contents, you will find approximately 17 different folders, all with the same file contents, but all of the files are encrypted with the algorithms listed on each folder's title, except the "Dummy Unencrypted Folder."

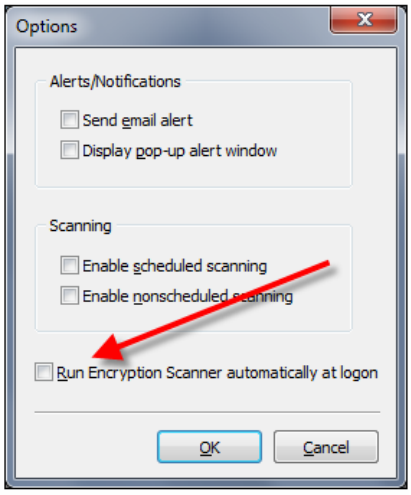
The "Dummy Unencrypted Folder" you can use on your PC or server, sharing it as a global network share to all of your users. Mapping a Drive Letter to the "Dummy Unencrypted Folder" is the preferred method of sharing this folder with all users.



Example Installation:

Let's say you have a Windows 2008 R2 file server and 10 users. Setup Encryption Scanner in this manner to protect your entire network:

1. Install Encryption Scanner on the Windows 2008 R2 file server. [see above instructions on installation.]
2. Create a folder called Dummy Files and share it on your network. Set the share permissions to "Everyone" or to all "Domain Users" in your department of business.
3. Either create a user Login Script or a Domain User Group Policy to map a drive letter [let's say drive letter "I:\"] to the Dummy Files share. Make certain that each user maps to the "I:\Dummy Files" mapped drive.
    a. As an alternative you can also use a UNC mapping like \\Windows2008Server\Dummy Files
4. In Encryption Scanner, setup your email address destinations for where the reports and alerts should be sent.
5. Make sure to check the Encryption Scanner Options and ensure that Encryption Scanner runs when the Windows 2008 server is rebooted for any reason

a. 

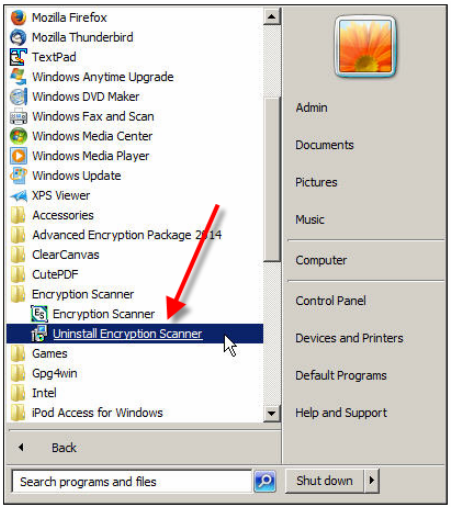
b. **THE ABOVE CONFIGURATION APPLIES TO THE DISPLAY APP ONLY**. For the Encryption Scanner 2.0 Service App configuration, see the Encryption Scanner 2.0 Service App Administration interface setup description earlier in this document.

6. Set the Encryption Scanner Timer interval for 5 minutes and click Start.
7. You are now Ready! The Encryption Scanner will scan the Dummy Files every 5 minutes. If a Crypto-Virus attacks any of your users, it will instantly infect the Dummy Files area and you will be alerted.

How to Uninstall Encryption Scanner

In most versions of Windows including XP, Vista, 7, and various Windows Server Editions, simply run the "Uninstall Encryption Scanner" icon from the Start Menu where applications are listed. You can also go to the Control Panel and either run Add/Remove Programs for XP or "Programs and Features" in Windows 7, 8; and run Uninstall from where Encryption Scanner is listed in the list of installed programs.

In some instances, a reboot may be required. Additionally, if you find that the Encryption Scanner 2.0 uninstaller has a conflict with existing anti-virus or other programs and is resistant to being uninstalled, even after a reboot, we recommend you download the free version of REVO UNINSTALLER.



Troubleshooting

Windows XP and .NET Framework 2.0 requirement:

When installing Encryption Scanner you may see a Setup Internal Error warning you that **".NET Framework version 2.0 is not installed."** You will need to install .NET Framework 2.0 first to complete the setup. You can download a copy of the .NET Framework 2.0 here: http://encryptionscanner.com/support/dotNetFX20.zip

Support, Disclaimer, and Copyright

Limited support is provided by email or by returned phone call appointment in the USA only.

If you need help with Encryption Scanner 2.0 installation or troubleshooting, send an email to support@encryptionscanner.com or call 760 489 9282 Monday thru Friday 9am – 5pm Pacific [Los Angeles] time.

Be sure to describe the trouble you are having and ensure that you have read our installation manual. Support is provided for licensed users only. Users using the trial version is available solely at the discretion of Tech Assist Inc.

Encryption Scanner is a product under copyright by Tech Assist Inc., a California Corporation, all rights reserved © 2014, 2015. See software license agreement before use. Unauthorized use and distribution will subject violator to extreme penalties under the law.

Tech Assist, Inc. assumed no liability for the failure of Encryption Scanner to run as advertised. Tech Assist, Inc. has done everything possible in testing to ensure that Encryption Scanner will run as advertised, but unforeseen events and the unknown affects of other software that may interfere with the Encryption Scanner's processes may cause a malfunction. Tech Assist, Inc. is hereby indemnified from all liability, and the user understands that using Encryption Scanner is totally at his/her own risk.